UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/661,589	09/14/2000	Blake Earl Hayward	P3953	9165

24739 7590 07/25/2008

CENTRAL COAST PATENT AGENCY, INC
3 HANGAR WAY SUITE D
WATSONVILLE, CA 95076

EXAMINER	
BRUCKART, BENJAMIN R	
ART UNIT	PAPER NUMBER
2146	
MAIL DATE	DELIVERY MODE
07/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/661,589
Filing Date: September 14, 2000
Appellant(s): HAYWARD, BLAKE EARL

Donald R Boys, Reg No. 35,074
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/16/08 appealing from the Office action mailed 2/19/08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

Claim 30, which is not mentioned, is also cancelled.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6496855	HUNT et al	12-2002
6910020	OYAMA et al	6-2005
6199113	ALEGRE et al	3-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim 29, 30-34, 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable by U.S. Patent No. 6,496,855 by Hunt et al.

Regarding claim 29, the Hunt reference teaches

a system for fraud prevention by authenticating a user at a first Internet site (Hunt: col. 2, lines 47-51 shows a user is verified; col. 4, lines 11-22, 30-41 teach protecting data for preventing fraud), comprising:

an Internet-connected verification server for performing the authentication (Hunt: col. 2, lines 36-51; the server); and

an Internet-connected appliance operable by the user for sending a request for authentication to the first Internet site (Hunt: col. 1, lines 56-61; the user; col. 5, lines 1-10; RAS);

wherein the user specifies sites not associated with the first Internet site known to the user as capable of accepting the user's username-password pair included in the request for authentication and a username-password pair for the user (Hunt: col. 2, lines 47-60; col. 6, lines

48-52; Fig. 1), and the server, in response to the request causes automatic navigation to sites and attempts a login on behalf of the user with the username-password pair, successful login at the sites allowing authentication of the user at the first Internet site (Hunt: col. 4, lines 1-5, 23-26).

The Hunt reference does not explicitly state a second and third Internet sites.

However, the Hunt reference does address the plurality of Internet sites that a user registers and authenticates with as a problem in which the invention is overcoming (Hunt: col. 1, lines 21-23, 30-35) in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54).

It would have been obvious at the time of the invention to one of ordinary skill in the art to create the system of fraud preventing by Hunt to include a second and third site that a client wishes to login as taught in the background of Hunt in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54).

Regarding claim 31, the system of claim 29, wherein the verification server is a first server, and the request is sent from the appliance to a second server on the network, which forwards at least a portion of the request to the first server, and the first server returns an indication of verification after causing the navigation and log-in attempt to the second and third sites provided by the user (Hunt: col. 2, lines 36-60; first server is target web server; second server is registration agent server; col. 8, lines 39-42).

Regarding claim 32, the system of claim 29, wherein all or a portion of the request is compared against stored user profile data for verification purposes (Hunt: col.3, lines 31-40; col. 2, lines 47-51).

Regarding claim 33, the system of claim 29, wherein the request comprises at least three or more user specified network destination sites and username-password pairs for the sites, and authentication is a number based on log-in results (Hunt: col. 6, lines 48-52; col. 8, lines 43- col. 9, line 15; Fig. 1).

Regarding claim 34, the Hunt reference teaches

a method for fraud prevention by authenticating a user at a first Internet site (Hunt: col. 2, lines 47-51 shows a user is verified; col. 4, lines 11-22, 30-41 teach protecting data for preventing fraud), comprising the steps of:

(a) accepting by a server an authentication request from the user comprising at least a plurality of Internet sites known to the user as capable of accepting the user's username-pair for each site and the username-password pairs are included in the authentication request from the user (Hunt: col. 2, lines 47-60; col. 6, lines 48-52);

(b) causing, by the server, automatic navigation to the sites and an automatic login attempt on behalf of the user with the username-password pairs (Hunt: col. 4, lines 1-5, 23-26); and

(c) reporting an indication of authenticity of the user according to success or failure of the login attempts (Hunt: col. 8, lines 39-42).

The Hunt reference does not explicitly state a second and third Internet site.

However, the Hunt reference does address the plurality of Internet sites that a user registers and authenticates with as a problem in which the invention is overcoming (Hunt: col. 1, lines 21-23, 30-35) in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54).

It would have been obvious at the time of the invention to one of ordinary skill in the art to create the system of fraud preventing by Hunt to include a second and third site that a client wishes to login as taught in the background of Hunt in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54).

Regarding claim 36, the method of claim 34 wherein the server is a first server, and the request is sent from the appliance to a second server on the network, which forwards at least a portion of the request to the first server, and the first server returns and indication of authenticity after causing the navigation and log-in attempt at the sites provided by the user (Hunt: col. 2, lines 36-60; first server is target web server; second server is registration agent server; col. 8, lines 39-42).

Regarding claim 37, the method of claim 34 wherein all or a portion of the request is compared against stored user profile data for verification purposes (Hunt: col.3, lines 31-40; col. 2, lines 47-51).

Regarding claim 38, the method of claim 34, wherein the request comprises three or more sites and username-password pairs for the Internet sites, and authentication is a number based on log-in results (Hunt: col. 6, lines 48-52; col. 8, lines 43- col. 9, line 15).

(10) Response to Argument

The examiner maintains the rejection because the Hunt reference does teach the claimed limitations.

Preamble. With respect to the preamble, Appellant argues the Hunt reference fails to teach a fraud prevention system as claimed.

Hunt teaches 'a system for fraud prevention by authenticating a user at a first Internet site' in col. 2, lines 47-51 and col. 4, lines 11-22, 30-41. Hunt teaches preventing fraud by utilizing a third party proxy login system for registration and repeated login to sites. The first site is the website in which the "registration agent site provides … to complete registration forms for websites by proxy and logging into their sites on repeat visits." Fraud is interpreted to be "intentional deception." Hunt clearly teaches a fraud prevention system by the proxy controlling access to the email address and protecting the users email address from being used as spam.

First limitation. With respect to the first limitation, Appellant argues Hunt does not teach "an Internet-connected verification server for performing the authentication."

The Hunt reference does teach the limitation, specifically in col. 2, lines 36-40 where Hunt teaches each service computer or server node is internet connected. The Hunt reference teaches the registration agent computer or registration agent server (RAS) also is connected to the internet. Lines 46-51 of Hunt teach verifying a user identity and password. Fig. 5 confirms this notion with the requirement of login before the RAS can transfer site login details.

Second limitation. With respect to the second limitation, Appellant argues Hunt does not teach "an Internet-connected appliance operable by the user for sending a request for authentication to the first Internet site."

The Hunt reference does teach the limitation specifically in col. 1, lines 56-61 and col. 6, lines 1-10. Col. 1 is relied upon to show a user who is interactive and involved with the fraud prevention system. The user fills in private and personal data as indicated in col. 6. The RAS system is an internet-connected appliance operated on by the user for repeatedly logging into other sites. See Fig 5 for the flow of events in which a user logs into the RAS before sending requests to authenticate to other websites.

Third Limitation and Motivation. With respect to the third limitation, Appellant argues the Hunt reference does not teach "wherein the user specifies a second and third Internet site not associated with the first Internet site and known to the user as capable of accepting the user's username-password pair included in the request for authentication and a username-password pair for the user, and the server, in response to the request, causes automatic navigation to the second and third site sites and attempts a login on behalf of the user with the username-password pair, successful login at the second and third sites allowing authentication of the user at the first Internet site."

Appellant brings further attention to the "successful login at the second and third sites allows authentication of the user at the first Internet site."

The first Internet site is the targeted web site that the user wishes to register or be authenticated at (col. 8, lines 15-19). The second and third sites are the sites that confirm the identity such as a RAS site (col. 8, lines 39-46). This coincides with the dependent claims 31, and 36 in which the navigation server attempts to log in to verification sites before allowing authentication a first site.

The Hunt reference's teachings render the claim limitation unpatentable. Hunt teaches a user specifying sites not associated with the first Internet site in col. 2, lines 47-60 and col. 6, lines 48-52 because the Hunt reference shows a user logs into a first site, the RAS system, and then registers or logs into other sites specified by the user through data structures and forms as

initiated/entered by the user in col. 6. The other websites are known to the user as capable of accepting requests for authentication because the user's id-password pair associated with other sites has already been registered with the corresponding web service or site.

The server which is interpreted to be 'an internet-connected verification server' in response to the request, which is interpreted to be the request for authentication, causes automatic navigation to sites and attempts a login on behalf of the user with the id-password pair is taught by Hunt is the one of the most rudimentary features of the invention. Hunt teaches col. 4, lines 1-5, 23-26 the RAS server "logging into sites on repeat visits" so the user doesn't have to retype all the information. The act of logging in by proxy is the "caused navigation" to the other sites for attempted login.

The examiner has admitted Hunt does not teach all the claim limitations in a 102 interpretation but that the broad claim limitations are unpatentable as an obvious variation of Hunt.

As evidence previously cited in the case prosecution and teaching a state of the art, the Alegre reference teaches a user logging into a trusted network with a username/password pair that is then sent to a third party entity, the authentication server, for verification. Thus sending username/password pairs for verification is already known in the art (Alegre: col. 4, lines 24-34).

Further evidence teaching a state of the art and also previously cited, the Oyama reference teaches a user applying for a bank account a first bank with bank account information of a second bank. The first bank verifying the second bank account by confirmation (Oyama: col. 2, lines 36-54).

The Hunt reference does not explicitly state a second and third Internet sites.

However, the Hunt reference does address a plurality of Internet sites that a user registers and authenticates with as a problem in which the invention is overcoming (Hunt: col. 1, lines 21-23, 30-35 and Fig. 1) in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54). Hunt teaches using a RAS server to verify and register a user who wishes to log into a first site. The RAS contains many profiles associated and policies detailing the information allowed to be shared of the user.

It would have been obvious at the time of the invention to one of ordinary skill in the art to create the system of fraud preventing by Hunt to include a second and third site that a client

wishes to login as taught in the background of Hunt in order to protect user data and privacy with the growth number of sites a user registers with (Hunt: col. 1, lines 21-54). The motivation to extend the proxy login to additional sites is given both in classification and idea of the prior art (proxy authentication and proxy login by third party systems for fraud prevention) as well as non-explicit embodiments where other web services and web sites are shown (Fig. 1, background).

Regarding claim 34, appellant provides similar arguments to those outlined above. The examiner maintains the rejections on all claims, specifically claims 34 for the same reasons as cited above.

The dependent claim arguments are directed to contain no newly argued features than those mentioned above and are not patentable for the same reasons argued above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Benjamin R Bruckart/
Examiner, Art Unit 2146

Conferees:

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2146

/Jason D Cardone/
Supervisory Patent Examiner, Art Unit 2145